Station Setup Guide to Access OMIE Information Systems

Alfonso XI, 6
28014 Madrid
F(+34) 91 524 03 96
www.omie.es

Ref. GuiaConfAccesoSistemasOMIE_Eng.docx

Version 2.1
Date: 2012-11-23

ÍNDICE

1	**INTRODUCTION**	**3**
2	**PRE-REQUISITES**	**4**
2.1	MAIN COMPONENTS AND VERSIONS	4
2.2	OPERATING SYSTEM	5
2.2.1	*Screen setup*	*5*
2.2.2	*User Account Control*	*5*
2.3	MICROSOFT INTERNET EXPLORER	6
2.4	JAVA VIRTUAL MACHINE FROM SUN	9
2.5	CARD READER INSTALLATION (ONLY FOR SMARTCARD CERTIFICATES)	11
2.6	USER CERTIFICATE REGISTRATION	11
2.6.1	*Smartcard certificates*	*11*
2.6.2	*Software certificates*	*13*
2.7	SIGNING ENTITY CERTIFICATE (OMIE ROOT CA CERTIFICATE)	15
3	**AUTOMATIC INSTALLATION OF COMPONENTS**	**19**
3.1	FIRST SYSTEM ACCESS	19
3.2	COMPONENTS UPDATE	23
4	**SIGNATURE APPLET SETUP**	**24**
5	**FREQUENT PROBLEMS**	**26**
5.1	ERROR MESSAGES APPEAR DURING INSTALLATION OF APPLETS	26
5.2	THE CARD PIN REQUEST TAKES A LONG TIME, OR THE BROWSER STALLS	27
5.3	"SECURITY ALERT" APPEARS ON LOGGING ONTO THE SYSTEM	28
5.4	THE SERVER DOES NOT ALLOW ACCESS TO THE SYSTEM	28
5.5	USE OF *NAMESPACES* IN XML DOCUMENTS (ONLY FOR ELECTRICITY MARKET WEBSITE)	29
5.6	BLOCKING POP-UP WINDOWS	30
5.7	PROBLEMS WHEN DOWNLOADING COMPONENTS	32
5.8	FILE DOWNLOAD WARNING	33
5.9	PROBLEMS STARTING DOWNLOAD CENTER (ONLY FOR THE ELECTRICITY MARKET WEBSITE)	33
5.10	PROBLEMS LOGGING ONTO THE WEB WITH NO JAVA INSTALLED	34
5.11	INCORRECT INSTALLATION OF OMEL ROOT CA CERTIFICATE	35
5.12	TWO WINDOWS OF THE DOWNLOAD CENTER ARE OPENED (ONLY FOR THE ELECTRICITY MARKET WEBSITE)	36

1 INTRODUCTION

This guide describes the requirements for a client station to access OMIE Information Systems and the necessary steps to start using the Web environments of the Electricity Market's Information System (hereinafter SIOM).

SIOM websites require *Microsoft Internet Explorer* browser and *Sun's Plug-in* for running Java components in the browser. Likewise, it is required to access using user certificates provided by OMIE, either on smartcard or file (software certificate) support

There are no sections on the installation of hardware and standard software components, such as the operating system, browser, or the hardware installation of the card reader. However, the following paragraphs outline the necessary requirements as regards versions and some setup details for the same to ensure proper working. For the basic installation of products, you should consult their installation or help guides.

2 PRE-REQUISITES

2.1 Main components and versions

The main software and hardware components required for the SIOM Web Sites are the following:

- Operating system:
  - Windows XP Home / Professional, SP2 or higher
  - Windows 7 (recommended)
- Microsoft Internet Explorer browser
  - Versions 8 (with disabled compatibility view) and 9 (recommended), both for 32 bits
  - Auctions Web sites allow also Internet Explorer 7
- Sun Java Virtual Machine
  - Versions 1.6.0 update 30 ó higher (except versions 1.7)
  - Auctions Web sites allow also versions 1.6.0 from update 10

  In any case, the most up to date information about the latest recommended and approved version of the Virtual Machine for access to the SIOM websites is located on OMIE Public website (www.omie.es), on section “Technical documentation” inside “Trading System”.
- Card reader (only for smartcard certificates)
- User certificate registration
- OMIE Root CA Certificate

The following sections describe in more detail these requisites and additional configuration options.

2.2 Operating System

2.2.1 Screen setup

The website was designed for an optimal setup of **1280x1024 pixels and 65536 colours**.

2.2.2 User Account Control

Using Windows 7, it is necessary to launch the web browser as administrator or disable the security windows module “UAC” (User Account Control) for the first access to system for letting the installation of Java applets on the user station.

To disable UAC, go to:

Control Panel → User Accounts → User account control settings

Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify me when:
Programs try to install software or make changes to my computer
I make changes to Windows settings
Not recommended but can be selected if you use programs that are not certified for Windows 7 because they do not support User Account Control
Never notify

In this screen slide the slider bar to the lowest value (towards Never Notify), with description showing “Never notify me.”

This is the required setup for the first web access components installation. Once finished the installation and the first system access, UAC can be enabled again. It can be necessary to disable UAC again (see chapter 3.2) in case of updating the installed components,

Note: Screenshots of this document are taken on a Windows 7 system. For Windows XP systems follow the corresponding steps on that operation system.

2.3 Microsoft Internet Explorer

On Windows 7, 32 bits version of Internet Explorer web browser must be used.

On the other hand, given that the SSL (Secure Sockets Layer) protocol with strong encryption (128 or 256 bits) is used to establish a session, the browser must support this level of encryption. To check the level of encryption supported by the browser, just press the menu option "Help About Internet Explorer", and a screen similar to the following will display:

About Internet Explorer
Windows
Internet Explorer 8
Version: 8.0.7600.16385
Cipher Strength: 256-bit
Product ID: 55041-007-1825093-86148
Update Versions: 0
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
©2009 Microsoft Corporation
OK

Other configuration options to take into consideration are the following:

- Allow downloading of the signed Applets

  The browser is required to permit downloading of the signed Applets. To do so, you just have to select "**Medium-high**" for the security level in the "**Internet**" zone, which is the default security level setting on installing Internet Explorer. To check this setting, follow these steps from the browser menu:

  Tools → Internet options → Security

  From this screen, select the "**Internet**" zone and activate the "**Medium-high**" security level. In the event that the OMIE Website ("**.omie.es*") has been included in the "**Trusted sites**" zone, this zone must have "**Medium**" security level. In the case of the Electricity Market Web, the site "**.emergenciaomie.es*" must also be included as a trusted site.

  This security level is sufficient for most safe Web servers, and implies that downloaded components can be executed, though always with user confirmation.

  In case of having trouble entering the website, please check that the trusted sites configuration includes at least the following:

  - **Accessing SIOM and auctions websites:** "**.omie.es*"
  - **Accessing SIOME (backup SIOM website):** "**.emergenciaomie.es*"

- Allow the use of COOKIES

  Your browser must support COOKIES (small elements of information that the server stores in the client computer). The COOKIES of the OMIE Website Web interface are only used to control an active session.

  To allow the use of COOKIES, register the access URL in the "**Trusted sites**" zone, or select a medium security setting (which is the browser's default setting) for the internet zone in:

  Tools → Internet options → Privacy

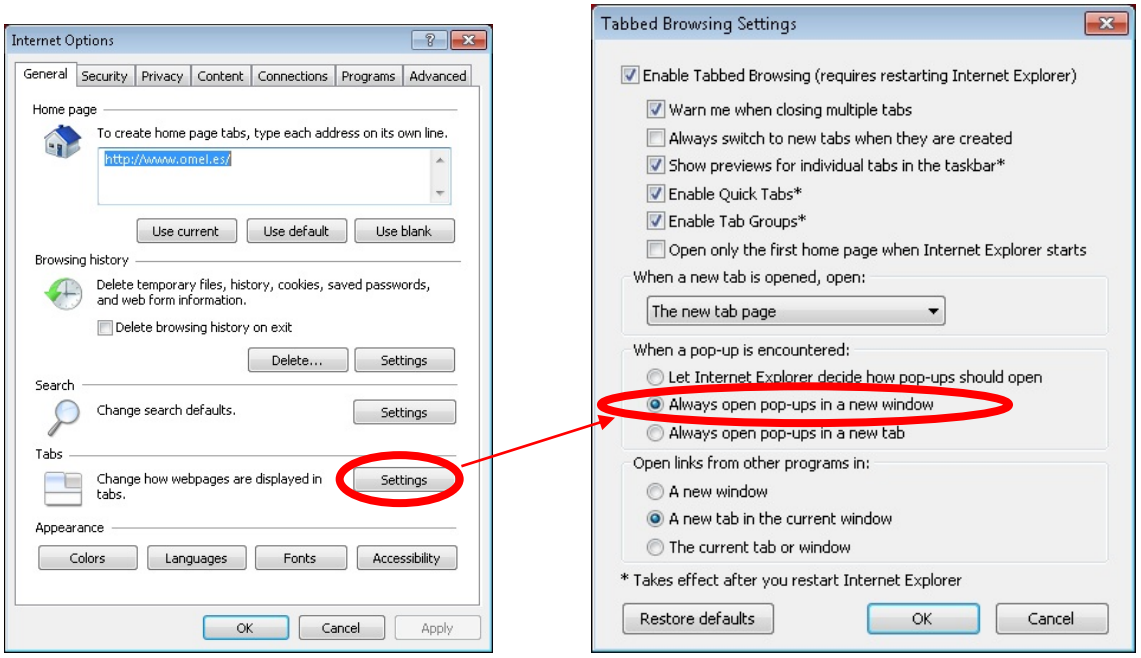
- Allow popup windows

  The browser must not block the SIOM website popup windows, as the said windows include the necessary functions for the correct working of the system. In the event that tools have been installed that block popup windows (for example, *MSN* or *Google* bars), or in the event that Windows XP SP2 (which adds privacy options allowing blocking of popup windows) is being used, you will need to configure the said tools so that the SIOM Web popup windows are not blocked.

  As regards this particular aspect, you are recommended to disable Blocking pop-up windows at least for all OMIE servers, by using the *"*.omie.es*" and "**.emergenciaomie.es*" masks and selecting low filter level (for further information, see section 5.6).

  In Internet Explorer 8 you are recommended to maintain the browser's default tab settings, so that the popup windows always open in a new window. The said settings are found in:

  Tools → Internet options → General → Tabs → Settings



- In Internet Explorer 9, disable ActiveX filtering

  Using Internet Explorer 9, it is required that the ActiveX filtering is disabled. Please check that this option is disabled on menu:

  Tools → ActiveX Filtering

- Enable editing through Excel (only for access to the Market website)

  If you wish to use the option for editing the content of bids through Excel (recommended for stations from which the bids are sent), you will need to modify the default setting of the "**Medium**" security level. At

  Tools → Internet options → Security → Internet

  Click on "**Custom level**" and look for:

ActiveX controls and plug-ins
Initialize and script ActiveX controls not marked as safe for scripting.
(✓)Prompt

  Although the default option is "**Disable**", you will need to mark "**Prompt**" or "**Enable**" in order to be able to launch Excel from the browser. This is due to the fact that Windows does not permit the Excel Active X (installed by Excel itself) to be marked as safe, as it has given rise to virus problems in the past.

  You are recommended to check the "**Prompt**" option (which implies that the browser requests the user confirmation to run the Excel ActiveX).

  For more information about the setup and working of the bid edit option through Excel, read the '**Excel Bid Editing, User Manual**'.

- Minimum options review

  For the case in which client security setup has already been customised due to the use of other applications, or to corporate security policies, indicated below are the **minimum options**, which must be activated for the correct use of the system (only the necessary options are described, those not listed do not affect the application). These values will be activated in the "Internet" zone, unless the OMIE Website has been included in one of the other zones (local intranet, trusted sites, restricted sites), in which case they will be activated in the corresponding zone.

  Tools → Internet options → Security → Internet

Scripting
Active scripting
(✓) Enable
Scripting of Java applets
(✓) Enable
ActiveX controls and plug-ins
Download signed ActiveX controls
(✓)Prompt [1]
Run ActiveX controls and plug-ins
(✓) Enable
Generate scripts of ActiveX controls marked as safe for scripting
(✓) Enable
Downloads
File download
(✓) Enable[2]

  As for **advanced setup** options, the following option must be selected:

  Tools → Internet options → Advanced options

Security
[✓] Use SSL 3.0

[1] *Necessary for downloading applets to the client on first accessing the application.*

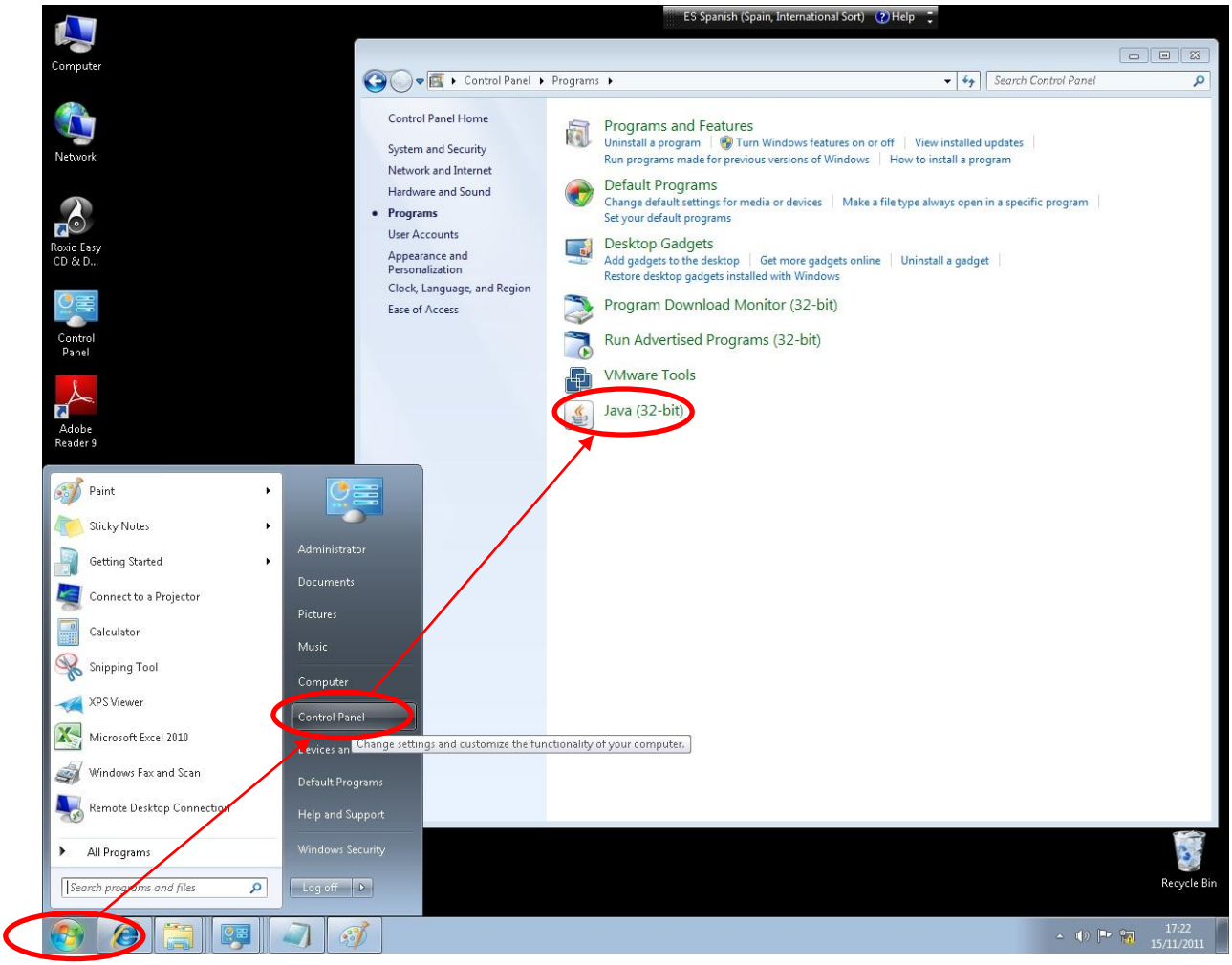
[2] *Necessary for downloading bids and other data to a file.*

2.4 Java Virtual Machine from Sun

OMIE's website interface makes intensive use of executable components which are downloaded from the web server. These components are Java programs, also known as Applets, which have been previously signed by OMIE so that the browser can check their authenticity to ensure that execution of the same does not lead to any security problem.

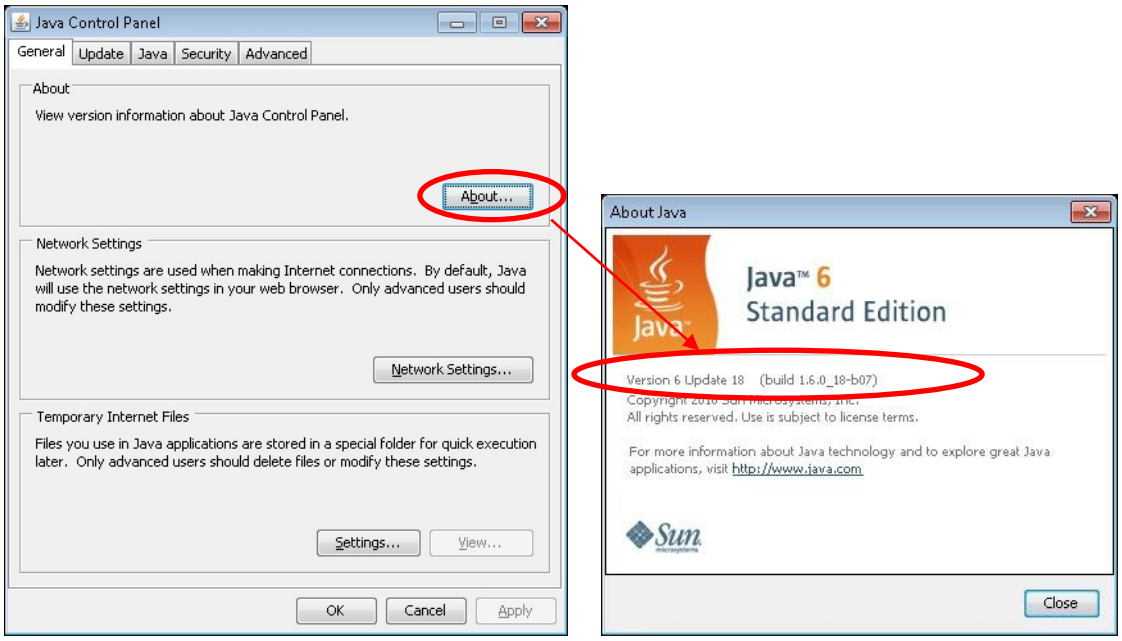
Because of that, you must install and activate the browser's Java virtual machine (JVM, which is the Applet execution environment. The required JVM is the one provided by Sun. The browser uses the said virtual machine through an extension or Plug-in, which is installed together with the JVM

To check if this JVM is installed, see if the "Java" option exists in the Windows Control Panel:



In the event that the said option is not available, you must install Sun JVM. To do so, log onto the SIOM website and activate the download from there (see instructions below).

If a Sun JVM is already installed, to check its version, start the Java Control Panel, and click on the “About” button:


Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings...
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings...
View...
OK
Cancel
Apply
About Java
Java™ 6
Standard Edition
Version 6 Update 18 (build 1.6.0_18-b07)
All rights reserved. Use is subject to license terms.
For more information about Java technology and to explore great Java applications, visit http://www.java.com
Close

If the version is not valid, update by removing the installed version and access OMIE’s website. From there, and as described in Chapter 3, the correct JVM will automatically be installed, without the need to previously download any version of the said virtual machine (in order to carry out this installation, the user connected to the operating system is required to have the necessary Administrator privileges).

The current version must be removed from the “Add or remove programs” option in the Windows Control Panel, by selecting entry-J2SE Runtime Environment with the corresponding version, and by clicking on Remove.

Chapter 3 describes the way to install the correct JVM from the OMIE website.

***Note**: Updating the JVM version can be carried out through the options available in the Update tab in the Java Control Panel, or by downloading the latest version from the Sun website. However, in order to avoid installing versions which have not yet been certified for use in SIOM, you are recommended to carry out the installation by accessing the website with no virtual machine installed.*

2.5 Card reader installation (Only for smartcard certificates)

In order to access SIOM Websites, a X.509 personal security certificate it's needed, which OMIE issues on a Gemplus smart card or file. In case of using a certificate issued in a smartcard a smart card reader is needed.

The user can use any standard PC/SC compatible reader, in which Gemplus software must be installed. The **'Gemplus software installation guide'**, which is provided as a separate document, outlines the steps to be followed. The card reader must be previously installed and you must be able to use the security card with Internet Explorer in order to be able to follow the steps listed below for setting up the station.

If you wish to install a GemPCTwin card reader, the specific drivers for this card reader will need to be installed once the Gemplus software has been installed.

2.6 User certificate registration

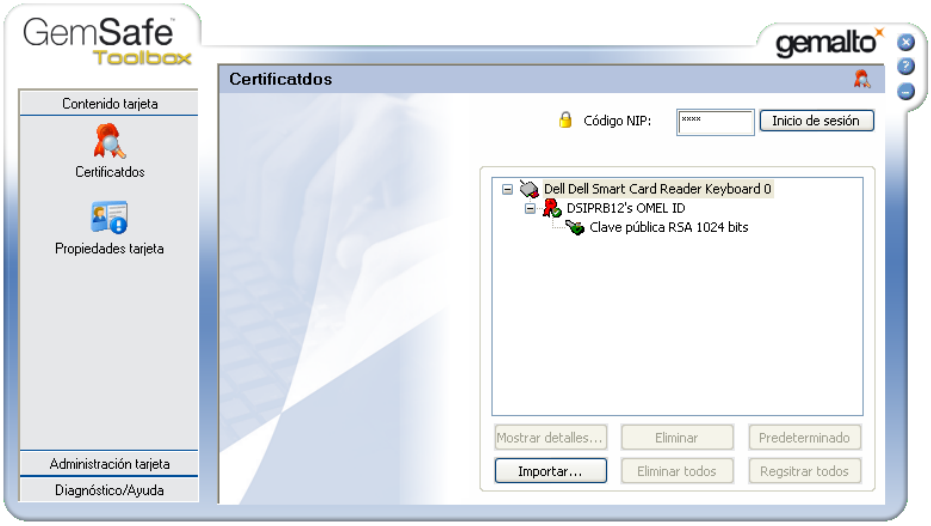
2.6.1 Smartcard certificates

When using a new security card for the first time at a user station, keep in mind that you **will need to register with Windows the certificate** stored in the card so that it can be used from the browser (it is a requirement of Internet Explorer). In Windows XP this registration is carried out automatically under certain conditions, although you are recommended to do it manually in all cases in order to ensure the correct working with different users and profiles on the same PC.

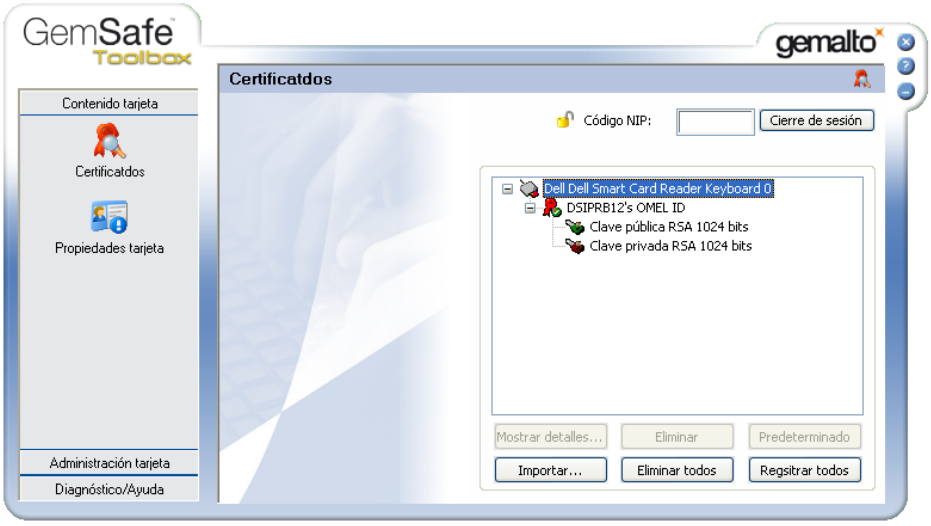
Use the Card reader software to register a certificate, as follows:

Insert the card in the reader and start the *GemSAFE Toolbox* program from Windows:

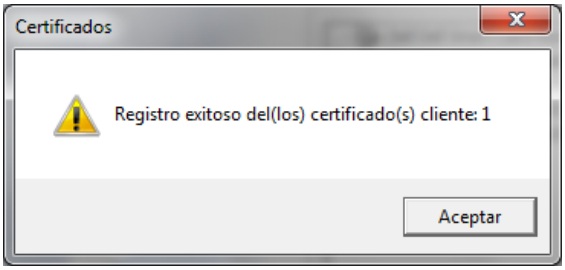
Click on *Card contents* → *Certificates* (Contenido tarjeta → *Certificados)* and enter the card PIN in the *NIP Code* section. Click on the *Start session* button to start the session:



To register the certificate, select the card icon and click on *Register all (Registrar todos)*:



The following screen will display after a few seconds indicating that the certificate has been registered.



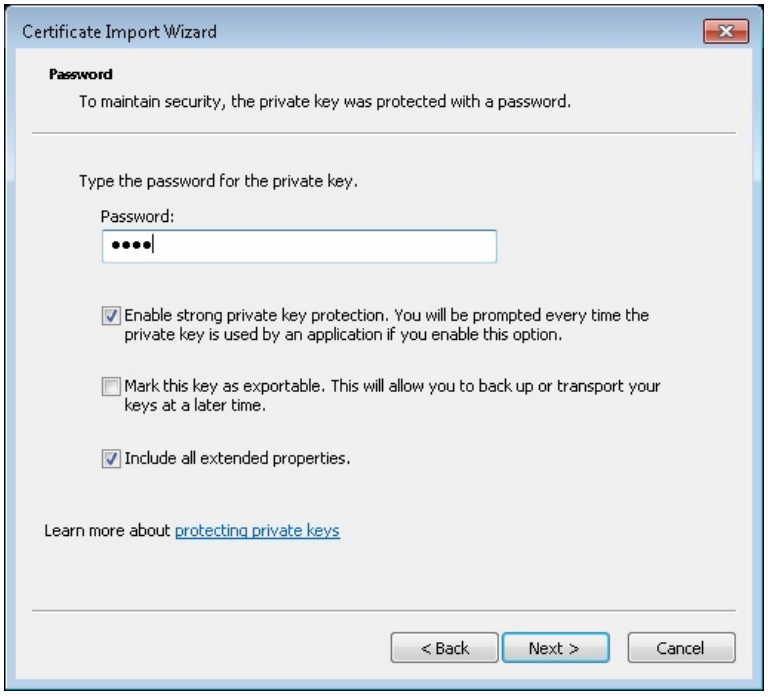
Click *Accept (Aceptar)* to finish the process of registration of the certificate.

2.6.2 Software certificates

File support certificates a.k.a. software certificates, are issued on ".p12" file (PKCS #12 standard). For registering issued software certificates, follow the next steps.

Download ".p12" file in an accessible location from the station where software certificate is going to be registered. Select the file with double click (this process can be started from the web browser too in "*Tools / Internet options / Content / Certificates / Import*")

Follow the given steps showing in the screen using the default options until this window is shown:


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about protecting private keys
< Back
Next >
Cancel

Type OMIE's issued private key password and check "Enable strong private key protection" box.

Follow with default options until this window is shown:

Click on “Set security level…”

Choose a Security Level
Choose a security level appropriate for this item.
High
Request my permission with a password when this item is to be used.
Medium
Request my permission when this item is to be used.
< Back
Next >
Cancel

In this window, “Medium” or “High” level can be selected for setting up system behaviour when using certificate to SIOM access or information sent signing. Selecting “Medium” browser only will show a confirmation window when private key access is needed. Selecting “High”, browser will request the password for the private key access.

It’s recommended to select “High” level and choose a password as a PIN for system access and data sent signing. Doing this, this window will appear after clicking “Next” for typing and confirm the chosen password:

Alter clicking on “Finish” and “OK”, this window will mean the end of the process:

2.7 Signing entity certificate (OMIE Root CA Certificate)

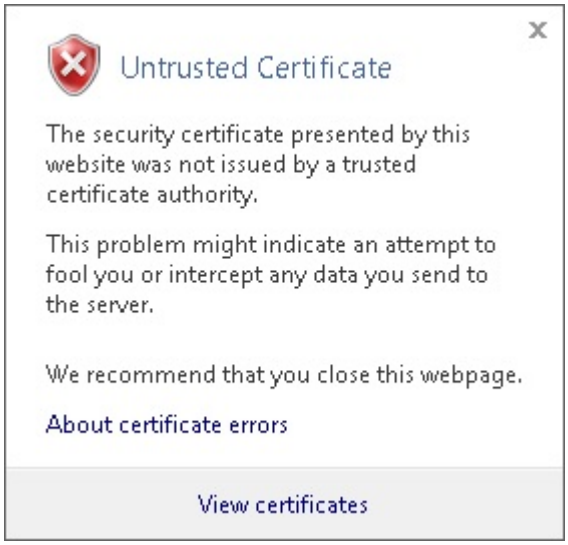
An indispensable requisite for the correct installation of components typical of SIOM Webs is having the OMEL CA Signing Entity certificate installed in the browser. The steps for installing the OMEL CA certificate are outlined below.

When accessing the system for the first time, or whenever the said certificate is not installed, the following warning screen will display. At the said screen, click on "**Continue to this website**":

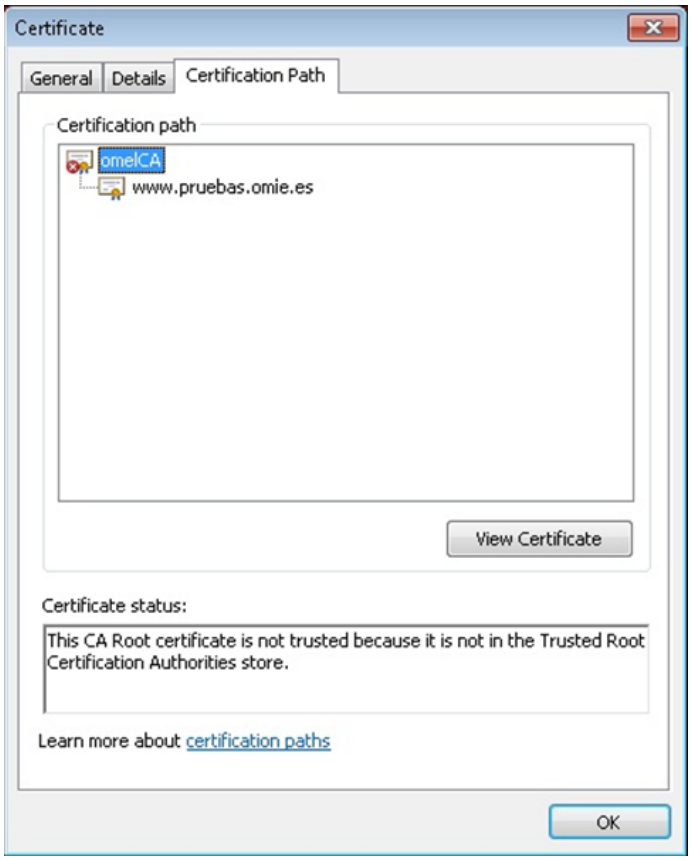
Certificate Error: Navigation Blocked - Windows Internet Explorer
https://www.pruebas.omie.es/
Favorites
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Then click on "**Certificate error**" which displays on the right hand side of the address bar:

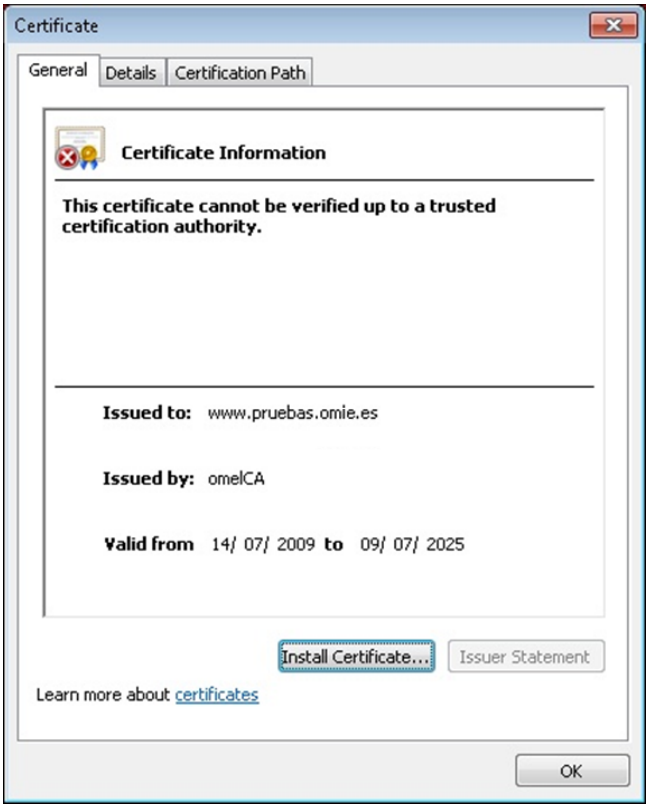
This window will display. Click on "**View certificates**":


Untrusted Certificate
The security certificate presented by this website was not issued by a trusted certificate authority.
This problem might indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage.
About certificate errors
View certificates

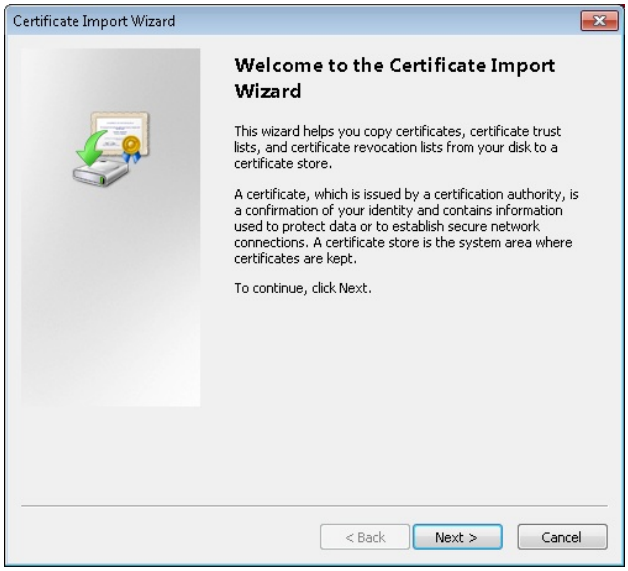
In the next window, click on the third tab (Certification Path). Select the tree root (omelCA) and click on "**View Certificate**":



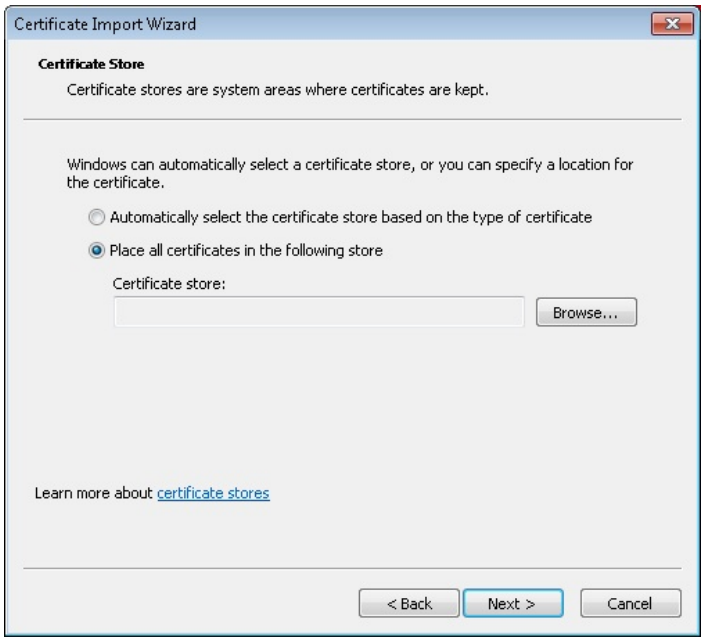
At the next window, click on "**Install certificate**":



Click on “**Next**”:

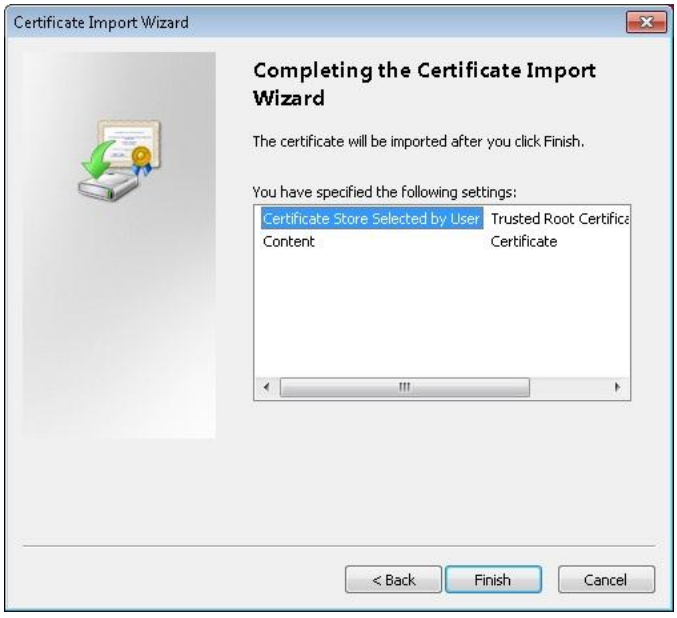

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

At the next window, check option “**Place all certificates in the following store**” and click on “**Browse**”

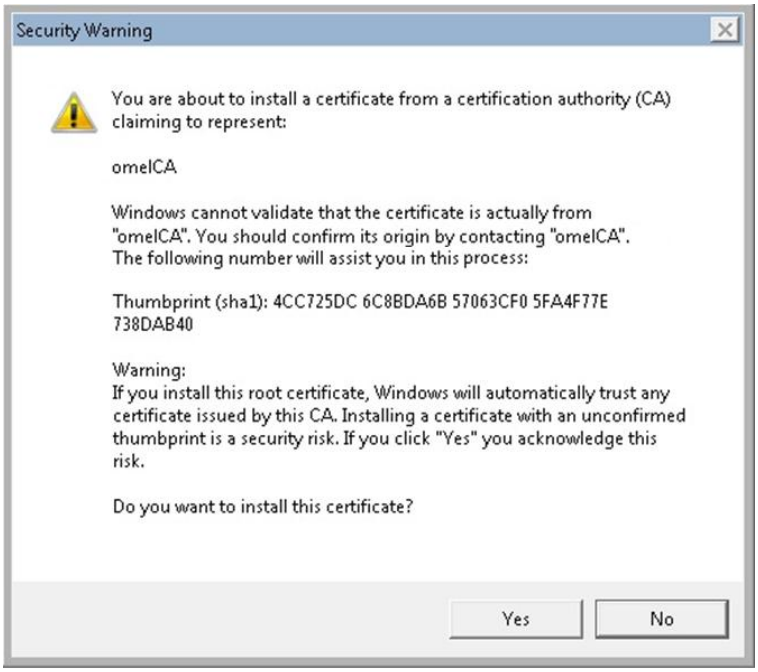

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

At the next window, select “**Trusted Root Certification Authorities**” and click on “**OK**”.

On the previous window click on “**Next**”, and once the next window opens, select “**Finish**”:



Then the next window opens where you click on “**Yes**” to finish the certificate import:


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
omelCA
Windows cannot validate that the certificate is actually from "omelCA". You should confirm its origin by contacting "omelCA". The following number will assist you in this process:
Thumbprint (sha1): 4CC725DC 6C8BDA6B 57063CF0 5FA4F77E 738DAB40
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

The browser confirms the correct installation of the certificate. Click on “**OK**”:

3 AUTOMATIC INSTALLATION OF COMPONENTS

3.1 First system access

On accessing the system for the first time, the necessary components or applets are installed in the local hard drive. For correct installation, on this first occasion you will need to be the computer's **local administrator** or if using Windows 7, disable UAC (see chapter 2.2)

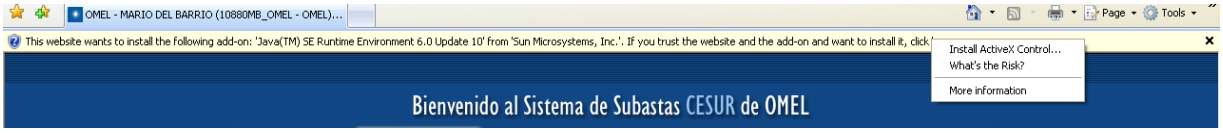
The steps for installing the components are outlined below:

- Access without an installed Java Virtual Machine

  Go to the website (for instance, www.mercado.omie.es). At this page, the JVM activates verification and downloading of the system's Applets. However, if no version of Sun's JVM has been installed, a window will display asking whether you wish to install the latest supported version (the shots show version 1.6.0_30)

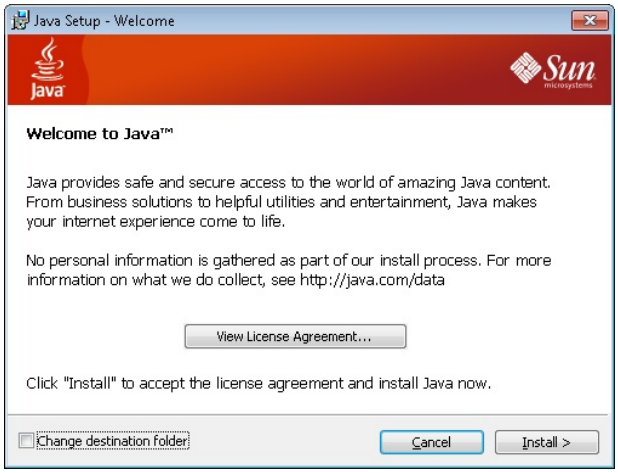
Internet Explorer - Security Warning
Do you want to install this software?
Name: Java(TM) SE Runtime Environment 6.0 Update 30
Publisher: Sun Microsystems, Inc.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

  From Internet Explorer 8, the installation process starts from a message that displays on the upper part of the browser, indicating whether that it is necessary to install a new "ActiveX control" (in Explorer 8), which is the JVM itself, or that there is certain blocked content (in Explorer 9).

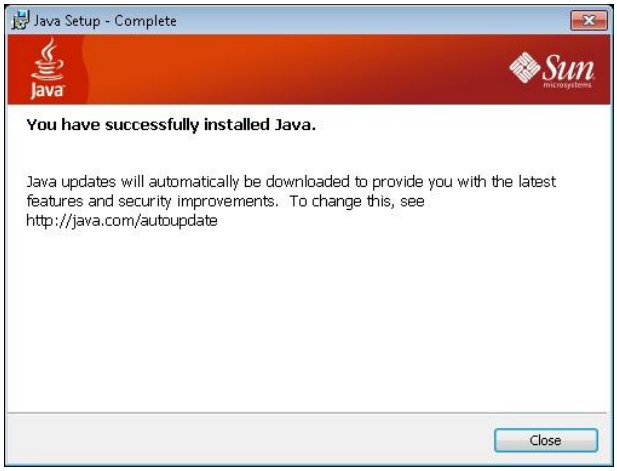

OMEL - MARIO DEL BARRIO (10880MB_OMEL - OMEL)...
This website wants to install the following add-on: 'Java(TM) SE Runtime Environment 6.0 Update 10' from 'Sun Microsystems, Inc.'. If you trust the website and the add-on and want to install it, click
Install ActiveX Control...
What's the Risk?
More information
Bienvenido al Sistema de Subastas CESUR de OMEL

  After clicking on "Install" or "Display Blocked Content" (depending on the browser), the installation process of the same will start, as described below. In order to complete this installation process, the user connected to the operating system requires Administrator privileges.

Several installation screens display until the process has been completed:

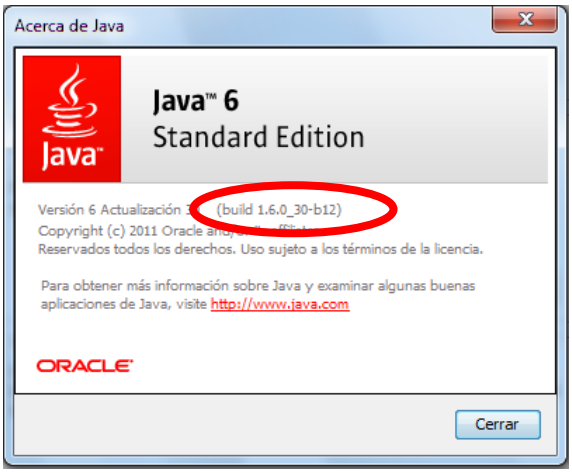

Java Setup - Welcome
Welcome to Java™
Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life.
No personal information is gathered as part of our install process. For more information on what we do collect, see http://java.com/data
View License Agreement...
Click "Install" to accept the license agreement and install Java now.
Change destination folder
Cancel
Install >

Java Setup - Progress
Installing Java
This may take a few minutes
Status: Extracting Installer
Now you can have a full-featured office suite that's compatible with Microsoft Office for free!
Powerful, integrated set of word processing, spreadsheet, presentation, drawing and database applications
Reads, edits and saves Microsoft Office files
Supports over 70 languages and Solaris, Windows, Linux and Mac operating systems
Uses industry-standard, open file format (OpenDocument) as its default file format
Built-in, one-click PDF export
OpenOffice.org

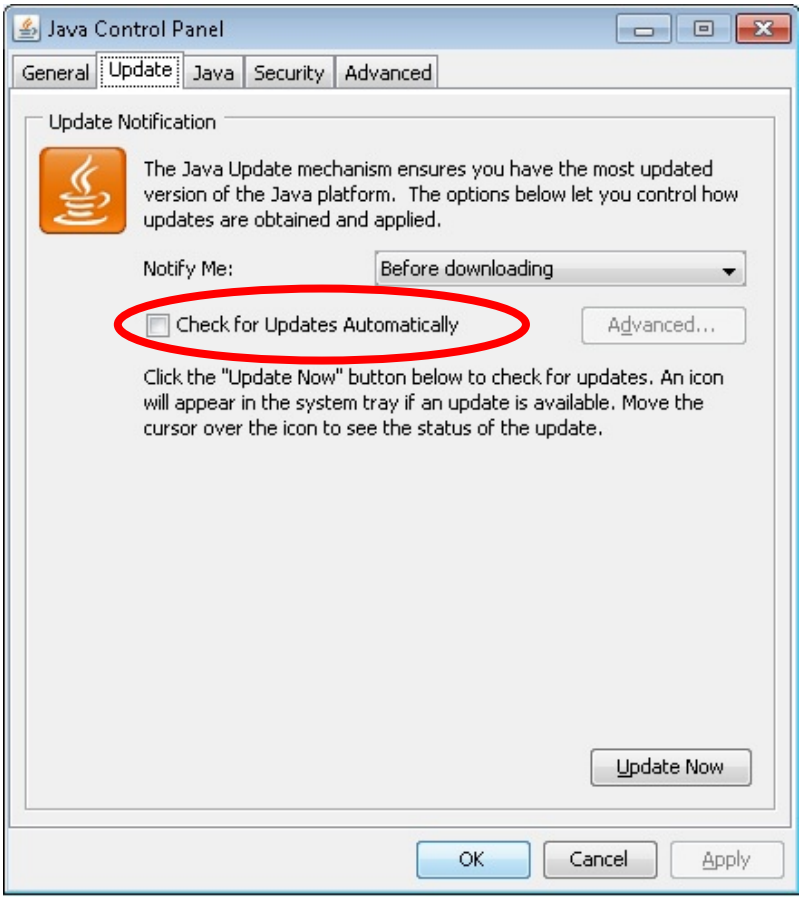

Java Setup - Complete
You have successfully installed Java.
Java updates will automatically be downloaded to provide you with the latest features and security improvements. To change this, see http://java.com/autoupdate
Close

***Note**: If you are using an installer other than the one that is run on accessing the SIOM Website, the option to install the so-called "Google bar" may display. In the event of its installation, keep in mind that it could cause interference in the control of opening pop-up windows from the SIOM application.*

To check the version of the recently installed JVM, you can once again consult the option "About" in the Java Control Panel:

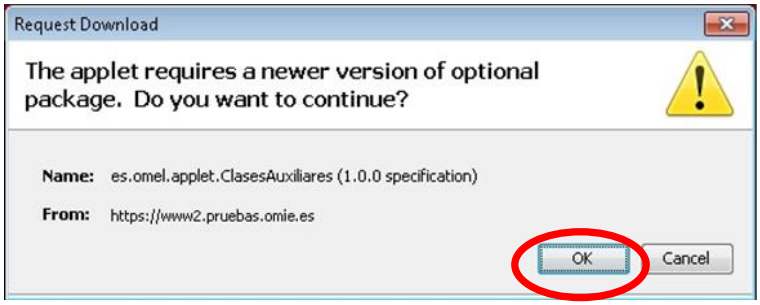

Acerca de Java
Java™ 6
Standard Edition
(build 1.6.0_30-b12)
Reservados todos los derechos. Uso sujeto a los términos de la licencia.
Para obtener más información sobre Java y examinar algunas buenas aplicaciones de Java, visite http://www.java.com
ORACLE
Cerrar

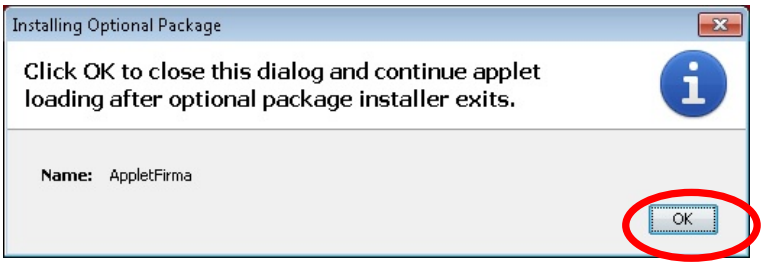
In addition, due to the possibility of Sun releasing a new version of JRE which has not yet been certified for use in SIOM, you are recommended to disable the automatic update of the JVM. This is configured by disabling the next box in the Java Control Panel:

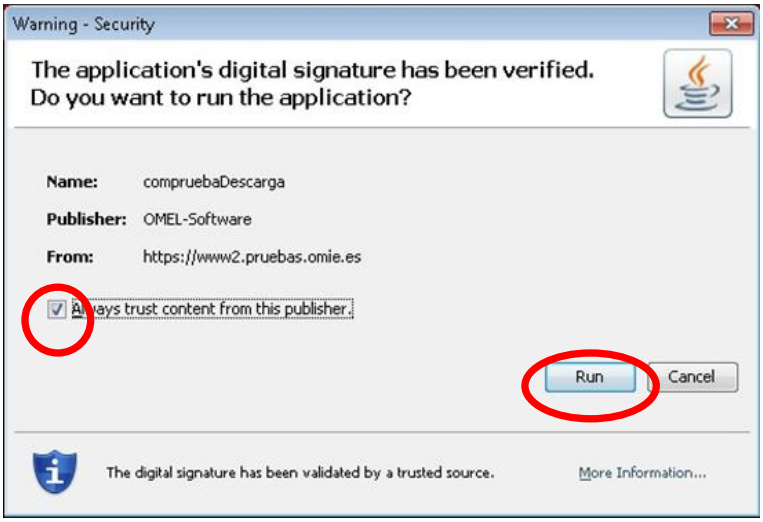

Java Control Panel
General
Update
Java
Security
Advanced
Update Notification
The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.
Notify Me:
Before downloading
Check for Updates Automatically
Advanced...
Click the "Update Now" button below to check for updates. An icon will appear in the system tray if an update is available. Move the cursor over the icon to see the status of the update.
Update Now
OK
Cancel
Apply

- Installation of system Applets

  Then the verification and downloading of the system's Applets is enabled. During download, you cannot enter the system. To confirm the download and execution of the applets, several screens similar to the following will display.


Request Download
The applet requires a newer version of optional package. Do you want to continue?
Name: es.omel.applet.ClasesAuxiliares (1.0.0 specification)
From: https://www2.pruebas.omie.es
OK
Cancel


Installing Optional Package
Click OK to close this dialog and continue applet loading after optional package installer exits.
Name: AppletFirma
OK


Warning - Security
The application's digital signature has been verified. Do you want to run the application?
Name: compruebaDescarga
Publisher: OMEL-Software
From: https://www2.pruebas.omie.es
Always trust content from this publisher.
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

In all cases, click OK, until all the packages have been installed. In the event of a security warning, mark the "Always trust content from this publisher" box so that this warning does not appear in the future.

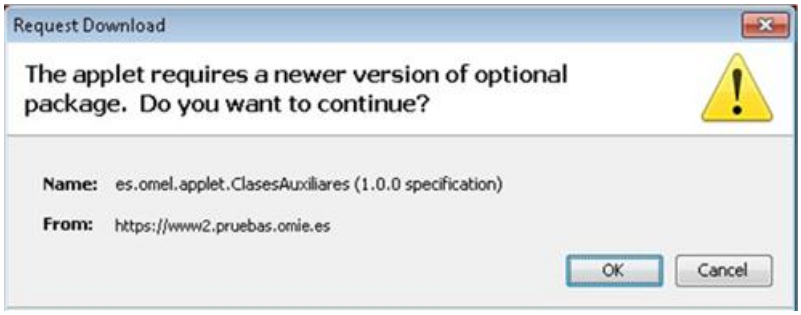
At this point the installation has concluded and the user can browse as normal through the Web. Once the components has been installed, a normal user, without administration privileges, can normally log into the system.

***Note**: In the event that Sun's JVM version is updated in the PC, the download and automatic installation of components process is repeated when the website is entered agan.*

***Note**: This download is expected to take place from "omie.es" domain, since it is an initial installation and configuration process that should only be done the first time the PC connects to SIOM. For that reason, in the case of the Market Website, such download will not be completed successfully if the first connection occurs while market operation is performed on the backup website.*

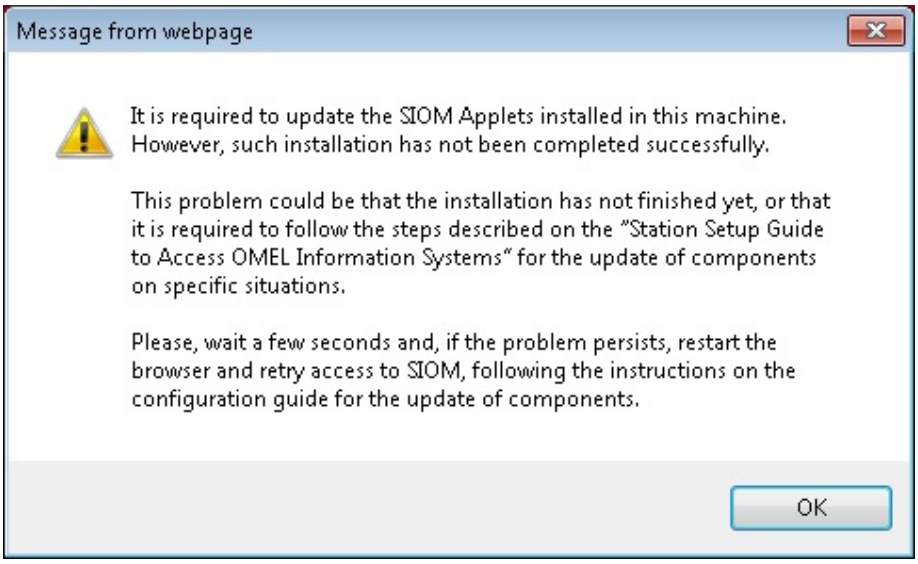
3.2 Components update

When some local components installed in the station are update by OMIE the web browser will repeat the steps described in the first installation automatically, showing few windows like the following:


Request Download
The applet requires a newer version of optional package. Do you want to continue?
Name: es.omel.applet.ClasesAuxiliares (1.0.0 specification)
From: https://www2.pruebas.omie.es
OK
Cancel

After clicking “OK” new applet will be installed and normal access to system will be completed.

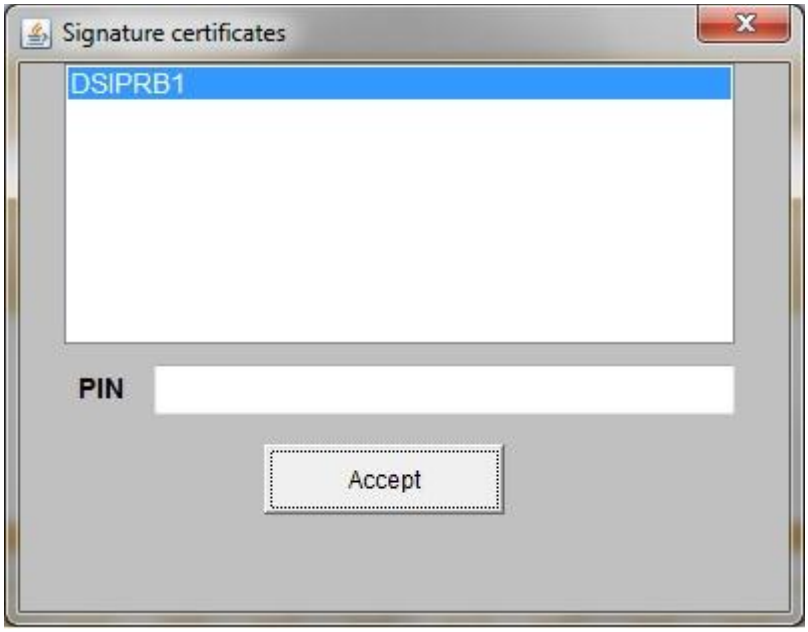
If any problem happens during update, this window will be shown:


Message from webpage
It is required to update the SIOM Applets installed in this machine. However, such installation has not been completed successfully.
This problem could be that the installation has not finished yet, or that it is required to follow the steps described on the “Station Setup Guide to Access OMEL Information Systems” for the update of components on specific situations.
Please, wait a few seconds and, if the problem persists, restart the browser and retry access to SIOM, following the instructions on the configuration guide for the update of components.
OK

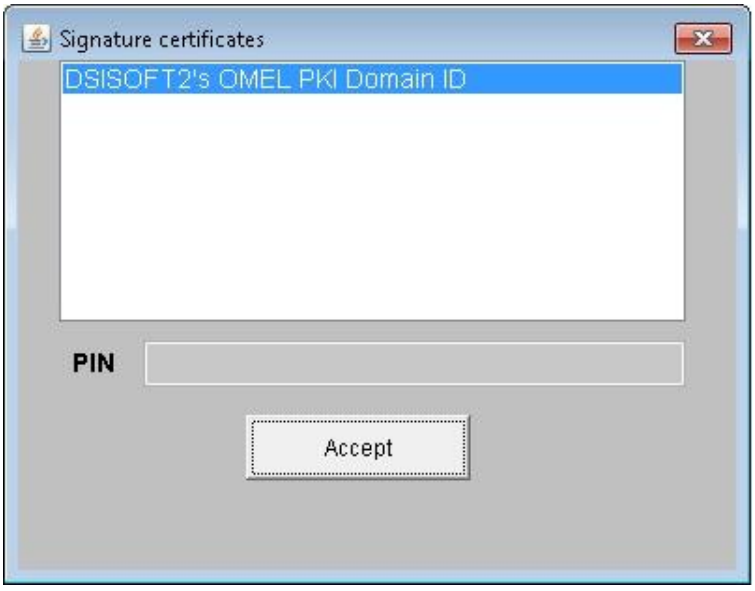
This problem may be happening because Windows 7 is being used and UAC (User Account Control. See chapter 2.2) is enabled. Please disable UAC for components updating and re-enable it when completed.

4 SIGNATURE APPLET SETUP

The ‘Signature applet’ is the Java component used to send digitally signed information to OMIE. Its graphical view when any signed transmission is made is as follows:



This applet shows the certificate to use for digital signing data sents, that it’s the same certificate used for system connection. It also shows a field to type the certificate’s PIN in case a smartcard is being used. If a software certificate is being used this field will be disabled and it will be the web browser itself who will ask for the confirmation of using that certificate, with or without password according to the security level chosen in the first installation.



This ‘Applet’ has a setup file located in ‘**C:\OMEL\ConfAppletFirma.xml**’. The default ‘Applet’ establishes an initial configuration in the event that the said file does not exist, creating it for subsequent modification of the user. On the first installation of the station, this file will not be created until the website main page is accessed

The content of the said file is as follows:

```
<?xml version='1.0'?>
<!--
     NOTA : Cualquier cambio en este fichero se tendrá en cuenta a
            partir del próximo reinicio del navegador.
-->
<ConfAppletFirma>
     <Seguridad>
          <PINTimeout>0</PINTimeout>
     </Seguridad>
     <Log>

     <DirEnviosFirmados>c:\omel\EnviosFirmados</DirEnviosFirmados>
     </Log>
</ConfAppletFirma>
```

Two configurable parameters are established in this file:

- **PINTimeout**: PIN time-out. This time expressed in minutes establishes the maximum time that the Applet waits between the signed transmission in order to once again request the user PIN. If the maximum time defined has not passed between the signed transmission, the user will not be asked for the PIN again. The '0' value indicates that the user will always be asked for the PIN. This parameter has a maximum value established in 30 minutes. If set at a greater value, a default time of 30 minutes will be used.
- **DirEnviosFirmados**: Destination directory of the signed transmissions. A structure of subdirectories with all the signed transmissions made by the user with the 'Applet', will be created in this directory, organised by types of transmissions ("BidsMD", "ExecutionsCB", "BidsAuctions", "Claims Auctions", etc.). In the event that a non-existent directory is specified, the Applet will automatically create it. If the said directory cannot be created, the destination directory will be the one by default defined by the Applet, which is '**c:\omel\EnviosFirmados**'.

Any change in this file will not take effect until the browser is restarted.

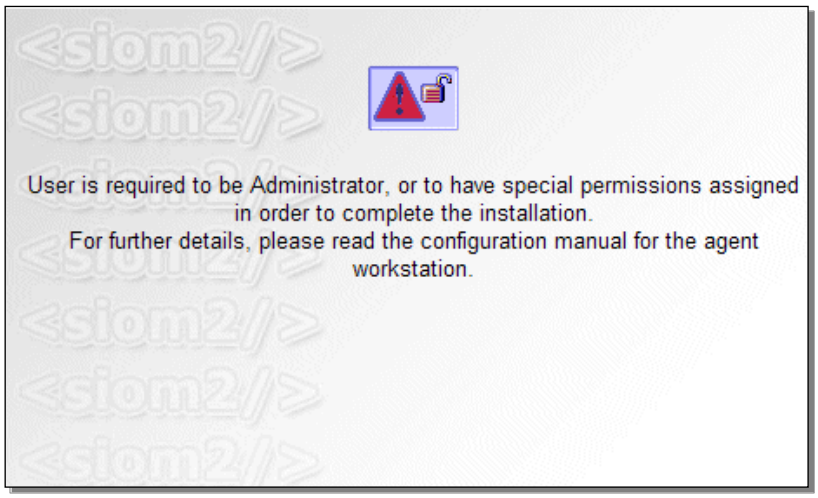
5 FREQUENT PROBLEMS

5.1 Error messages appear during installation of applets

When any of the following situations arise in Windows XP:

- The user who makes the first installation does not have administrator privileges,
- The Administrator did not give component update privileges to Advanced Users, and an Advanced User enters the system when OMIE has included an update of applet versions,
- A Normal User logs onto the system when OMIE has included an update of applet versions,

The browser main page will automatically close and the following message will display:

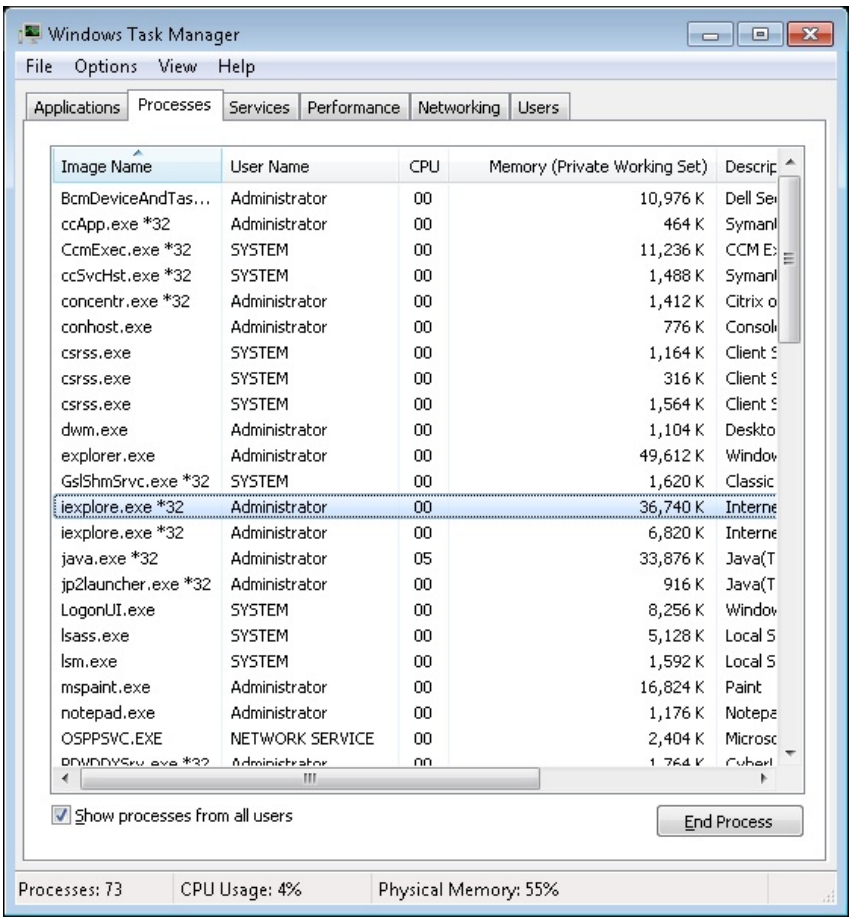

User is required to be Administrator, or to have special permissions assigned in order to complete the installation.
For further details, please read the configuration manual for the agent workstation.

To avoid this, access to the system must be made with a user with administrator privileges, or as an Advanced User if the Administrator has given privileges to Advanced Users to make subsequent updates.

5.2 The card PIN request takes a long time, or the browser stalls

This problem may be due to the fact that there are other Internet Explorer sessions open. To solve the problem, close all browser sessions, and repeat the entry to the system.

If the problem persists, check to see if there are processes active in the system Task Manager, under the name *IEXPLORE.EXE*, as shown in the image. In such an event, these processes must be manually closed from the Task Manager (by clicking on “End Process”), before trying to access to the system again.


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (Private Working Set) Descrip
BcmDeviceAndTas... Administrator 00 10,976 K Dell Se
ccApp.exe *32 Administrator 00 464 K Symanl
CcmExec.exe *32 SYSTEM 00 11,236 K CCM E
ccSvcHst.exe *32 SYSTEM 00 1,488 K Symanl
concentr.exe *32 Administrator 00 1,412 K Citrix o
conhost.exe Administrator 00 776 K Consol
csrss.exe SYSTEM 00 1,164 K Client S
csrss.exe SYSTEM 00 316 K Client S
csrss.exe SYSTEM 00 1,564 K Client S
dwm.exe Administrator 00 1,104 K Deskto
explorer.exe Administrator 00 49,612 K Windo
GslShmSrvc.exe *32 SYSTEM 00 1,620 K Classic
iexplore.exe *32 Administrator 00 36,740 K Interne
iexplore.exe *32 Administrator 00 6,820 K Interne
java.exe *32 Administrator 05 33,876 K Java(T
jp2launcher.exe *32 Administrator 00 916 K Java(T
LogonUI.exe SYSTEM 00 8,256 K Windo
lsass.exe SYSTEM 00 5,128 K Local S
lsm.exe SYSTEM 00 1,592 K Local S
mspaint.exe Administrator 00 16,824 K Paint
notepad.exe Administrator 00 1,176 K Notepa
OSPPSVC.EXE NETWORK SERVICE 00 2,404 K Microsc
Show processes from all users
End Process
Processes: 73 CPU Usage: 4% Physical Memory: 55%

5.3 “Security alert” appears on logging onto the system

As explained in section 2.7, this window opens when the OMEL CA Signing Entity certificate has not been registered in the browser.

Certificate Error: Navigation Blocked - Windows Internet Explorer
EN English (United States)
Help
https://www.pruebas.omie.es/
Bing
Favorites
Certificate Error: Navigation Blocked
Page
Safety
Tools
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

This can occur, even if the said certificate has already been registered, if you are using an operating system user that has not previously accessed the SIOM website or due to the update of the root CA in SIOM.

To solve this problem, follow the steps outlined in the present document, from section 2.7, onwards, and review the browser set up options for the user, as described in section **¡Error! No se encuentra el origen de la referencia.**.

5.4 The server does not allow access to the system

If error messages such as “*The page cannot be displayed*” or “*Access Forbidden*” appear, they may be due to the fact that you are using a browser that does not support 128-bit encryption.

To check the encryption level supported by the browser that you are using, follow the steps outlined in section 2.3.

Currently, the browser versions that can be downloaded from Microsoft have the necessary level of encryption. The problem may be due to the fact that an old version is being used, or one obtained when versions containing strong encryption and those that did not were differentiated for international legal reasons. Consequently, the problem is solved by installing an updated version of the browser.

5.5 Use of *Namespaces* in XML documents (only for Electricity Market website)

When XML documents which do not include the correct specification of the namespace are sent, either through the browser or through Web Services, an error message displays. In the case of transmission through the browser, a window with the following message displays:

A document parsing error has occurred:
The XML file does not have the correct namespace 'http://www.omel.es/Schemas'

For a XML document sent to OMIE to have the correct namespace, its header must include the contents as shown in the following example:

```
<MensajeOfertasMD xmlns="http://www.omel.es/Schemas">
  <IdMensaje v="OfertasMD-2004-10-05"/>
    <FechaMensaje v="2004-10-04T09:19:43-00:00"/>
    <IdRemitente v="AGENT"/>
  ...
</MensajeOfertasMD>
```

The error produced in the event of using a Web Service interface, taking as an example the forwarding of bids to the Daily Market, would be the following, which indicates that the server would be unable to find the element *'MensajeOfertasMD'* associated with the corresponding *Namespace*, within the document sent:

```
AxisFault
 faultCode:
   {http://xml.apache.org/axis/}Server.userException
 faultString:
   org.xml.sax.SAXParseException:
     Declaration not found for element 'MensajeOfertasMD'.
```

The *namespace* is used to avoid nomenclature conflicts between XML documents which could have the same labels with different purposes. With an aim to avoid possible future conflicts, strict appliance of standards and the specification of the *namespace* shall be obligatory in SIOM2*.*

Below are two examples of documents with nomenclature conflict:

Document with stock Exchange information:

```
<table>
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Document with product information:

```
<table>
  <name>American coffee table</name>
  <width>80</width>
  <length>120</length>
</table>
```

If these two types of document are aggregated in one document, there will be a conflict of elements as both documents contain the element *<table>.*

The use of *Namespaces* solves this type of problem by assigning a name space to a group of labels. *Namespaces* are usually defined in the XML document root, thus assigning this namespace to all the elements including children. Below are the two former XML documents which have been corrected to incorporate their *Namespace*:

Document with stock Exchange information:

```
<table xmlns="http://www.mibolsa.com/tabla">
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Document with product information:

```
<table xmlns="http://www.muebles.es/Catalogo">
  <name>American coffee table</name>
  <width>80</width>
  <length>120</length>
</table>
```

Due to the foregoing, all XML documents sent to OMIE and received from OMIE shall have the correct namespace to avoid possible conflicts.

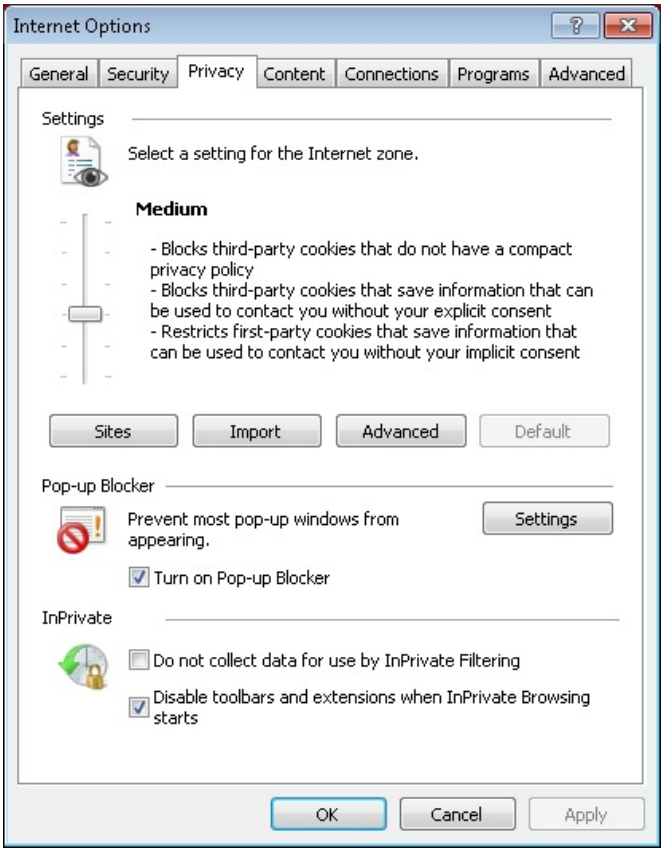
5.6 Blocking pop-up windows

The process for installing components of SIOM websites uses pop-up Windows to execute some of the steps (see chapter 3). In the event that popup windows are blocked in the browser, the said installation will not run correctly, and prevent operation in the web.

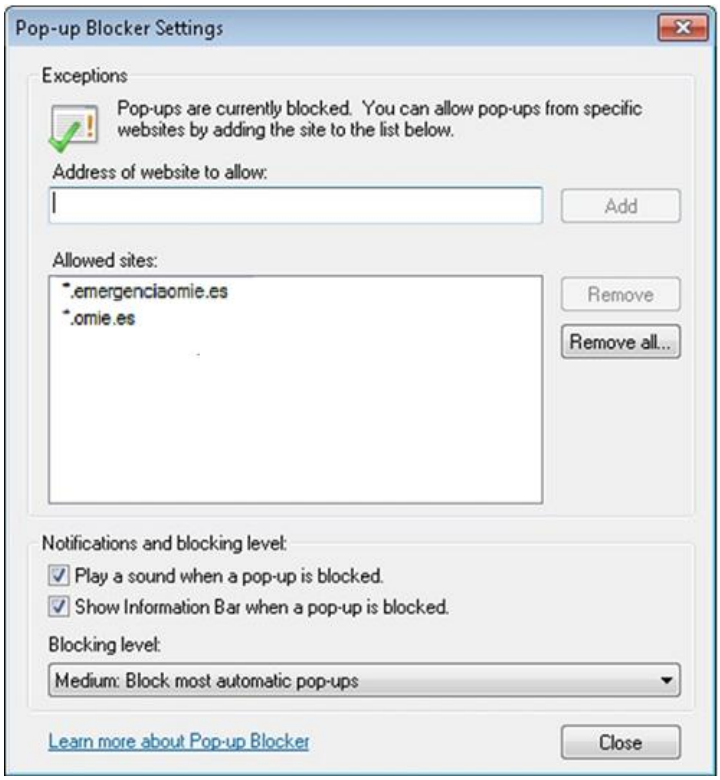
From Windows XP *Service Pack* 2 a modification is included in the *Internet Explorer* browser that allows the possibility of setting up Block pop-up windows. Below are some brief instructions on how to proceed in this case.

To configure block popup windows, do as follows

Tools → Internet Options → Privacy → Turn on Pop-up Blocker



If the "*Pop-up Blocker*" option is enabled, you won't be able to access SIOM correctly. To solve this problem, you must disable this option, or specify that OMIE's Web servers can open pop-up windows. To do so, click on "*Settings*", and the "A*ddress of website to allow*" text box and type "**.omie.es*" and click on "*Add*". In order to access the emergency environment without problems, the same configuration should also be made for "**.emergenciaomie.es*". In addition, you must specify as "*Filter level*" the option "*Low: Allow pop-ups from secure sites*" (see screen shot below).


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.
Address of website to allow:
Add
Allowed sites:
*.emergenciaomie.es
*.omie.es
Remove
Remove all...
Notifications and blocking level:
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Blocking level:
Medium: Block most automatic pop-ups
Learn more about Pop-up Blocker
Close

You will then have no problem in accessing all OMIE web servers.

In the event that the pop-up windows are blocked, and the OMIE windows have not been allowed, the following warning line may display in the browser, and the following options will display:

If you choose the "*Always allow pop-ups from this site*" option, the following confirmation window will display (example for the website "http://*www.pruebas.omie.es*"):

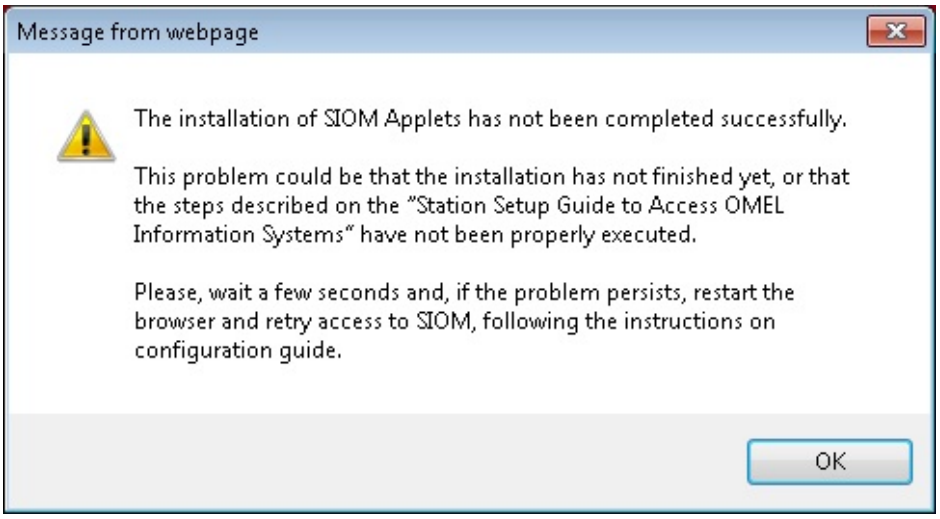
If you click on "*Yes*", the Block up windows will be disabled for this server, and you can make another attempt to access the website.

However, the first procedure described in this section is recommended, as it allows access to all OMIE servers with just one operation.

On the other hand, the blocking of pop-up windows can be enabled in other ways, such as for example by installing tools which, among other functions, allow the blocking of the said windows. This is the case of the *MSN* or *Google* bars (among others). In the event that one of these tools is installed, you will need to configure it so that OMIE web pop-up windows ("**.omie.es*" and "**.emergenciaomie.es*"), at least, are not blocked. To do so, check the documents provided by the said tools.

5.7 Problems when downloading components

If, after downloading components, there are any problems, when you click on the “ENTER” link the following message may display:


Message from webpage
The installation of SIOM Applets has not been completed successfully.
This problem could be that the installation has not finished yet, or that the steps described on the “Station Setup Guide to Access OMEL Information Systems” have not been properly executed.
Please, wait a few seconds and, if the problem persists, restart the browser and retry access to SIOM, following the instructions on configuration guide.
OK

If the problem persists after repeating the operation, after accepting all the downloads and after a reasonable time (which will depend on the speed of the connection), you can try the following operation.

- Close the browser
- Check the JVM version that is installed and active (there may be more than one version installed). To do so, run the “java –version” command in the command prompt window (*Start / All Programs / Accessories / Command Prompt*), and check the version that is displayed, for example:

```
java version "1.6.0_18"
Java(TM) SE Runtime Environment (build 1.6.0_18-b07)
Java HotSpot(TM) Client VM (build 16.0-b13, mixed mode, sharing)
```

- Remove all files with extension .JAR from the directory “*C:\Program files(x86)\Java\jre*[vers]*\lib\ext*” (where [vers] is the active version, which, in the previous example would be “6”), **except those belonging to the JVM** (currently, the said files are, for versions 1.6.0_xx: *dnsns.jar*, *meta-index, sunjce_provider.jar, sunmscapi.jar, sunpkcs11.jar* and *localedata.jar*).
- Repeat access to the Website, accepting all downloads.

If the problem is still not solved, it could be due to certain problems detected in the installation and removal of some versions of Java. To avoid these problems, take the following steps:

- Close the browser
- Remove the active Java version, and remove the “*C:\Program files(x86)\Java\jre*[vers]**” directory and its entire contents.
- Reinstall the required Java version or log on to the web so that the latest version supported by SIOM websites is installed.

5.8 File download warning

If you try to download a file (for example, download the request or response from a signed transactions enquiry), the following warning message may display:

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...
omie
08-10-2012 18:25:27

Although you indicate that you wish to download the file, the browser displays the web's main page.

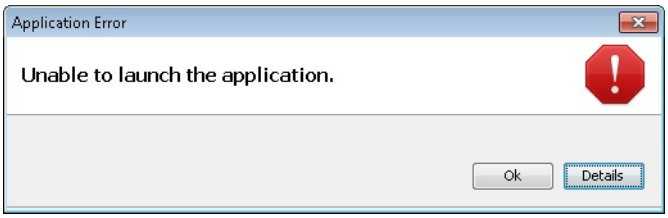
To solve this problem, you must make the following modification to the browser setup (as is indicated in section 2.3):

> *Tools / Internet options / Security / Internet [or zone in which the OMIE web is located] / Custom level / Downloads / Automatic prompting for file downloads / Enable.*

In this way, when requesting a file to be downloaded, the warning message will not display, and only the standard dialog box for opening it or saving it to disk will display.

5.9 Problems starting Download Center (only for the Electricity Market Website)

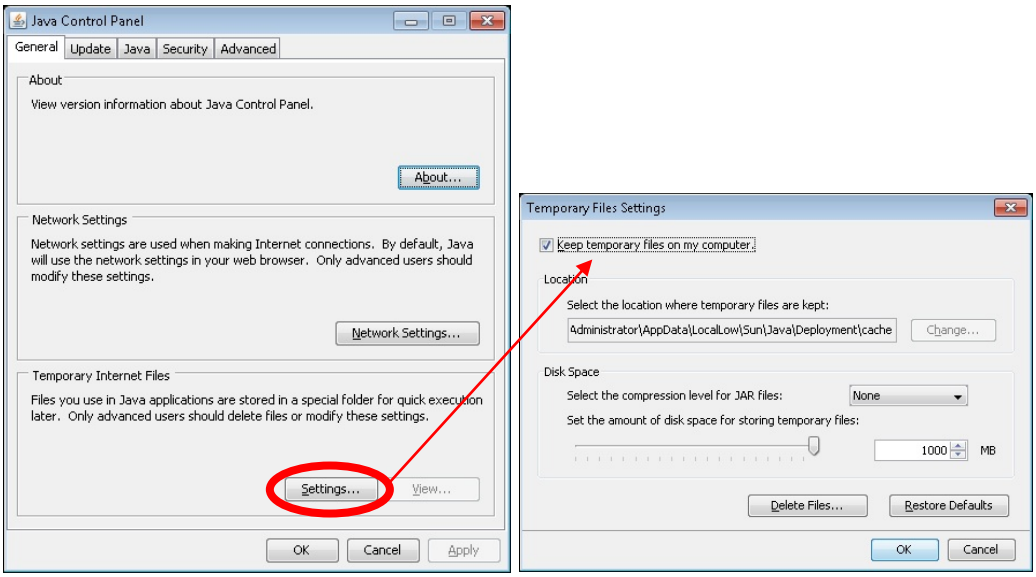
In some cases, after starting "Download Center" the following exception occurs:



This error is due to the incorrect configuration of JAVA, which prevents the application from booting. To solve this problem, change the settings from the control panel.

The said setup is found in:

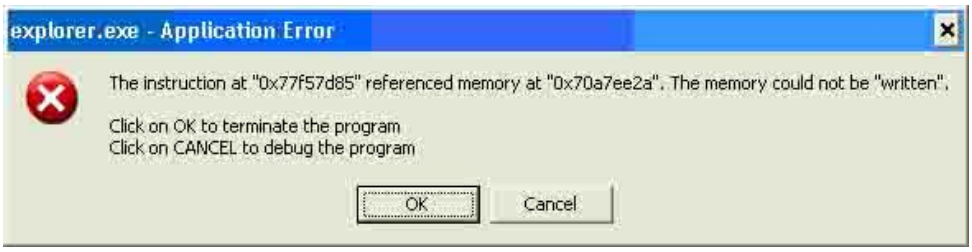
> *Control panel → Java → General → Temporary Internet Files → Settings*



From here, activate verification "Keep temporary files on my computer".

5.10 Problems logging onto the Web with no Java installed

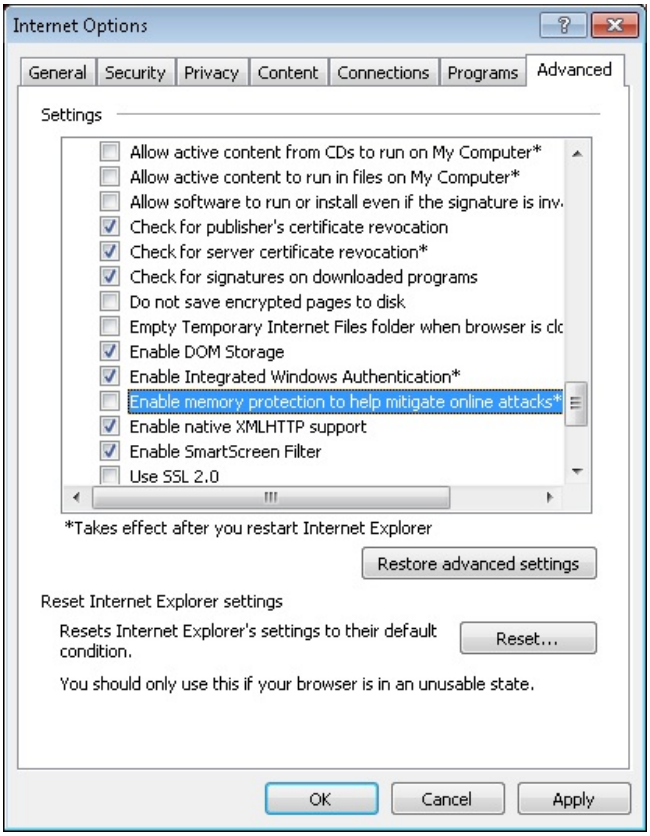
In some cases when logging on to the Web with IE8 and no Java JRE installed, the following error message displays:


explorer.exe - Application Error
The instruction at "0x77f57d85" referenced memory at "0x70a7ee2a". The memory could not be "written".
Click on OK to terminate the program
Click on CANCEL to debug the program
OK
Cancel

This error is due to a security mechanism incorporated in Explorer to avoid execution of malicious code ("*Data Execution Prevention*"). When installing JRE, just like in other browser extensions, this problem can arise if the said extensions are not updated for compatibility with this mechanism.

If you wish to carry out the installation from the Web, you can disable the verification as follows:

Tools → Internet Options → Advanced → Security


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Allow active content from CDs to run on My Computer*
Allow active content to run in files on My Computer*
Allow software to run or install even if the signature is inv
Check for publisher's certificate revocation
Check for server certificate revocation*
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is clc
Enable DOM Storage
Enable Integrated Windows Authentication*
Enable memory protection to help mitigate online attacks*
Enable native XMLHTTP support
Enable SmartScreen Filter
Use SSL 2.0
*Takes effect after you restart Internet Explorer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

Disable the "*Enable memory protection to help mitigate online attacks*" check box, reboot the browser and log on to the system again. You are recommended to reactivate this box after the installation process.

Another alternative is to download Java from the website itself;

http://java.sun.com/javase/downloads/index.jsp

Download the "JRE" version compatible with the application.

Once it has been downloaded, install as outlined in point 3.1 and then log onto the web again.

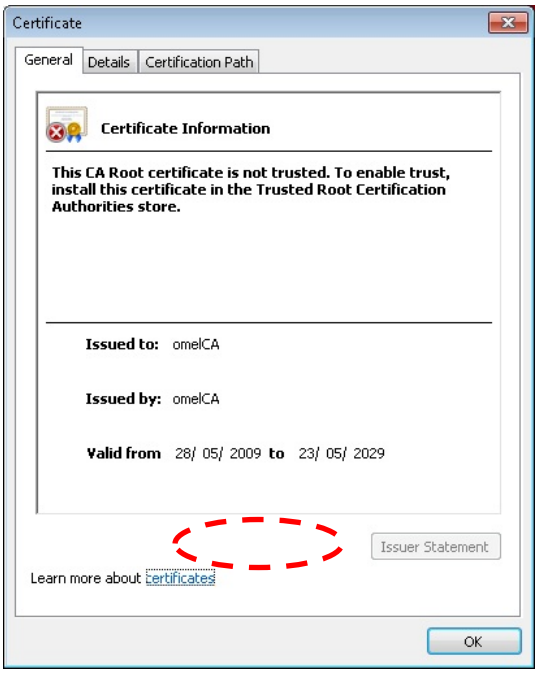
5.11 Incorrect installation of OMEL Root CA Certificate

It can happen that, after installation of OMEL Root CA Certificate, the security alert and the certificate error message are still displayed, and also the certificate error:

Certificate Error: Navigation Blocked - Windows Internet Explorer
EN English (United States) Help
https://www.pruebas.omie.es/
Favorites
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

This problem can be due to the fact that the OMIE Root CA Certificate has not been installed in the proper certificate store (if the browser default options are kept, the certificate can be installed in the "*Intermediate Certification Authorities*" store, instead of the "*Trusted Root Certification Authorities*" store).

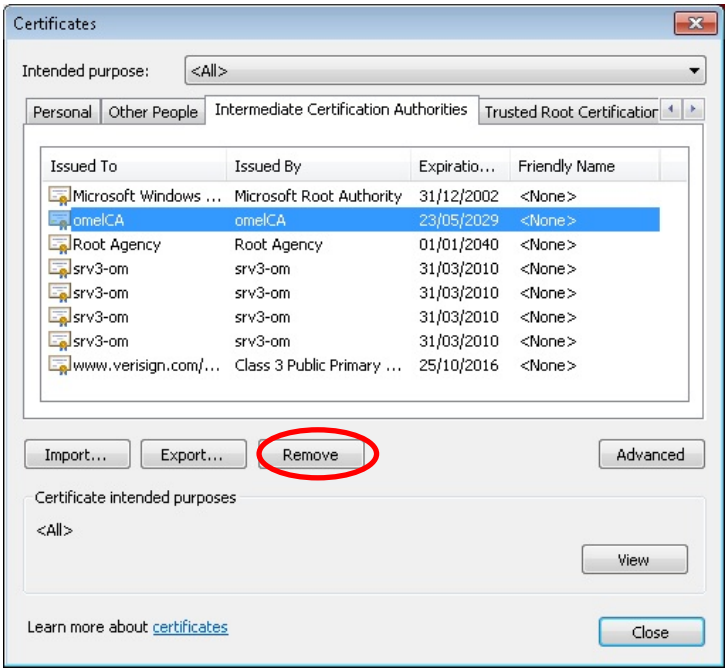
In Addition, in this situation it is not possible to install it again in the proper store, because if you follow the steps described on section 2.7, the button "Install certificate" does not appear. This is due to the fact that such certificate is already installed in a store.


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: omelCA
Issued by: omelCA
Valid from 28/ 05/ 2009 to 23/ 05/ 2029
Issuer Statement
Learn more about certificates
OK

Therefore, the solution is to uninstall the certificate first. In order to do so, you should enter from the browser into:

Tools → Internet Options → Content → Certificates → Intermediate Certification Authorities

From that point, you should select the "**omelCA**" certificate and click on "**Remove**".



After confirmation, the certificate should have been uninstalled. Then, you should follow the steps described on section 2.6 in order to properly install the OMEL Root CA Certificate.

5.12 Two Windows of the Download Center are opened (only for the Electricity Market website)

Sometimes, when you launch the Download Center from the Electricity Market website, it is started twice (two windows are opened, so the certificate is also requested twice).

This problem has been detected Internet Explorer 8 and 9, and with the "SmartScreen Filter" turned on. In order to solve this problem it is required to turn off this filter. The "SmartScreen Filter" can be found at:

Tools → SmartScreen Filter

Microsoft SmartScreen Filter
Help make your browser more secure:
Set up SmartScreen Filter
SmartScreen Filter is designed to warn you if the website you are visiting is impersonating another website or contains threats to your computer.
What is SmartScreen Filter?
Turn on SmartScreen Filter (recommended)
Some website addresses will be sent to Microsoft to be checked. Information received will not be used to personally identify you.
Turn off SmartScreen Filter
Website addresses will not be sent to Microsoft unless you choose to check them.
OK
Read the Internet Explorer Privacy Statement online.